

EXHIBIT A

LOCKS LAW FIRM, LLC

By: Michael A. Galpern, Esquire (Attorney No.: 029031988)

Andrew P. Bell, Esquire (Attorney No.: 025052010)

James A. Barry, Esquire (Attorney No.: 027512008)

801 N. Kings Highway

Cherry Hill, NJ 08034

Tel: (856) 663-8200

MORGAN & MORGAN COMPLEX LITIGATION GROUP

By: John A. Yanchunis, Esquire [To be admitted *Pro Hac Vice*]

Patrick Barthle, Esquire [To be admitted *Pro Hac Vice*]

201 N. Franklin Street, 7th Floor

Tampa, Florida 33602

Tel.: (813) 223-5505

Attorneys for Plaintiff and the Putative Class

GRANT MORROW on behalf of himself and other persons similarly situated,	SUPERIOR COURT OF NEW JERSEY LAW DIVISION: MIDDLESEX COUNTY
Plaintiffs(s)	DOCKET NO.: MID-L-7406-16
v. QUEST DIAGNOSTICS INCORPORATED; JOHN DOES 1-99 (fictitious entities) and XYZ CORPORATIONS 1-99 (fictitious entities),	Civil Action SUMMONS
Defendant(s)	

From The State of New Jersey, To the Defendant(s) Named Above:

QUEST DIAGNOSTICS INCORPORATED

The plaintiff, named above, has filed a lawsuit against you in the Superior Court of New Jersey. The complaint attached to this summons states the basis for this lawsuit. If you dispute this complaint, you or your attorney must file a written answer or motion and proof of service with the deputy clerk of the Superior Court in the county listed above within 35 days from the date you received this summons, not counting the date you received it. (A directory of the addresses of each deputy clerk of the Superior Court is available in the Civil Division Management Office in the county listed above and online at http://www.judiciary.state.nj.us/prose/10153_deptyclerklawref.pdf.) If the complaint is one in foreclosure, then you must file your written answer or motion and proof of service with the Clerk of the Superior Court, Hughes

Justice Complex, P.O. Box 971, Trenton, NJ 08625-0971. A filing fee payable to the Treasurer, State of New Jersey and a completed Case Information Statement (available from the deputy clerk of the Superior Court) must accompany your answer or motion when it is filed. You must also send a copy of your answer or motion to plaintiff's attorney whose name and address appear above, or to plaintiff, if no attorney is named above. A telephone call will not protect your rights; you must file and serve a written answer or motion (with fee of \$175.00 and completed Case Information Statement) if you want the court to hear your defense.

If you do not file and serve a written answer or motion within 35 days, the court may enter a judgment against you for the relief plaintiff demands, plus interest and costs of suit. If judgment is entered against you, the Sheriff may seize your money, wages or property to pay all or part of the judgment.

If you cannot afford an attorney, you may call the Legal Services office in the county where you live or the Legal Services of New Jersey Statewide Hotline at 1-888-LSNJ-LAW (1-888-576-5529). If you do not have an attorney and are not eligible for free legal assistance, you may obtain a referral to an attorney by calling one of the Lawyer Referral Services. A directory with contact information for local Legal Services Offices and Lawyer Referral Services is available in the Civil Division Management Office in the county listed above and online at http://www.judiciary.state.nj.us/prose/10153_deptyclerklawref.pdf.

/s/ Michelle M. Smith

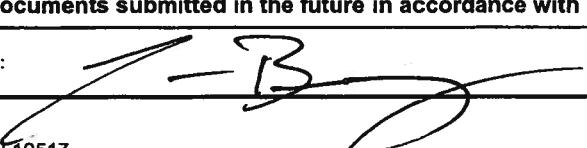
MICHELLE M. SMITH, Clerk
Superior Court of New Jersey

Dated: January 6, 2017

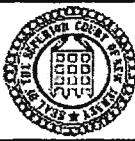
Name of Defendant to be Served: Quest Diagnostics Incorporated

Address of Defendant to be Served: Three Giralda Farms
Madison, NJ 07940

Appendix XII-B1

	CIVIL CASE INFORMATION STATEMENT (CIS)		FOR USE BY CLERK'S OFFICE ONLY PAYMENT TYPE: <input type="checkbox"/> CK <input type="checkbox"/> CG <input type="checkbox"/> CA CHG/CK NO. AMOUNT: OVERPAYMENT: BATCH NUMBER:
	Use for initial Law Division Civil Part pleadings (not motions) under Rule 4:5-1 Pleading will be rejected for filing, under Rule 1:5-6(c), if information above the black bar is not completed or attorney's signature is not affixed		
ATTORNEY / PRO SE NAME James A Barry		TELEPHONE NUMBER (856) 663-8200	COUNTY OF VENUE Middlesex
FIRM NAME (if applicable) Locks Law Firm		DOCKET NUMBER (when available) 2-7406-16	
OFFICE ADDRESS 801 Kings Highway North Cherry Hill, NJ 08034		DOCUMENT TYPE complaint	
		JURY DEMAND <input checked="" type="checkbox"/> YES <input type="checkbox"/> No	
NAME OF PARTY (e.g., John Doe, Plaintiff) Grant Morrow		CAPTION Grant Morrow v. Quest Diagnostics, Incorporated	
CASE TYPE NUMBER (See reverse side for listing) 508	HURRICANE SANDY RELATED? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	IS THIS A PROFESSIONAL MALPRACTICE CASE? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO IF YOU HAVE CHECKED "YES," SEE N.J.S.A. 2A:53 A-27 AND APPLICABLE CASE LAW REGARDING YOUR OBLIGATION TO FILE AN AFFIDAVIT OF MERIT.	
RELATED CASES PENDING? <input type="checkbox"/> YES <input checked="" type="checkbox"/> No		IF YES, LIST DOCKET NUMBERS	
DO YOU ANTICIPATE ADDING ANY PARTIES (arising out of same transaction or occurrence)? <input type="checkbox"/> YES <input checked="" type="checkbox"/> No		NAME OF DEFENDANT'S PRIMARY INSURANCE COMPANY (if known) <input type="checkbox"/> NONE <input type="checkbox"/> UNKNOWN	
THE INFORMATION PROVIDED ON THIS FORM CANNOT BE INTRODUCED INTO EVIDENCE.			
CASE CHARACTERISTICS FOR PURPOSES OF DETERMINING IF CASE IS APPROPRIATE FOR MEDIATION			
DO PARTIES HAVE A CURRENT, PAST OR RECURRENT RELATIONSHIP? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	IF YES, IS THAT RELATIONSHIP: <input type="checkbox"/> EMPLOYER/EMPLOYEE <input type="checkbox"/> FRIEND/NEIGHBOR <input type="checkbox"/> OTHER (explain) <input type="checkbox"/> FAMILIAL <input type="checkbox"/> BUSINESS		
DOES THE STATUTE GOVERNING THIS CASE PROVIDE FOR PAYMENT OF FEES BY THE LOSING PARTY? <input type="checkbox"/> Yes <input type="checkbox"/> No			
USE THIS SPACE TO ALERT THE COURT TO ANY SPECIAL CASE CHARACTERISTICS THAT MAY WARRANT INDIVIDUAL MANAGEMENT OR ACCELERATED DISPOSITION			
<input checked="" type="checkbox"/> Do you or your client need any disability accommodations? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		IF YES, PLEASE IDENTIFY THE REQUESTED ACCOMMODATION <input type="checkbox"/> P 3	
Will an interpreter be needed? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		IF YES, FOR WHAT LANGUAGE? <input type="checkbox"/> CIVIL OFFICE <input type="checkbox"/> MIDDLESEX <input type="checkbox"/> VICTORIANA	
I certify that confidential personal identifiers have been redacted from documents now submitted to the court, and will be redacted from all documents submitted in the future in accordance with Rule 1:38-7(b).			
ATTORNEY SIGNATURE: 			

Side 2



CIVIL CASE INFORMATION STATEMENT (CIS)

Use for initial pleadings (not motions) under Rule 4:5-1

CASE TYPES (Choose one and enter number of case type in appropriate space on the reverse side.)

Track I - 150 days' discovery

- 151 NAME CHANGE
- 175 FORFEITURE
- 302 TENANCY
- 399 REAL PROPERTY (other than Tenancy, Contract, Condemnation, Complex Commercial or Construction)
- 502 BOOK ACCOUNT (debt collection matters only)
- 505 OTHER INSURANCE CLAIM (including declaratory judgment actions)
- 506 PIP COVERAGE
- 510 UM or UIM CLAIM (coverage issues only)
- 511 ACTION ON NEGOTIABLE INSTRUMENT
- 512 LEMON LAW
- 801 SUMMARY ACTION
- 802 OPEN PUBLIC RECORDS ACT (summary action)
- 999 OTHER (briefly describe nature of action)

Track II - 300 days' discovery

- 305 CONSTRUCTION
- 509 EMPLOYMENT (other than CEPA or LAD)
- 599 CONTRACT/COMMERCIAL TRANSACTION
- 603N AUTO NEGLIGENCE - PERSONAL INJURY (non-verbal threshold)
- 603Y AUTO NEGLIGENCE - PERSONAL INJURY (verbal threshold)
- 605 PERSONAL INJURY
- 610 AUTO NEGLIGENCE - PROPERTY DAMAGE
- 621 UM or UIM CLAIM (includes bodily injury)
- 699 TORT - OTHER

Track III - 450 days' discovery

- 005 CIVIL RIGHTS
- 301 CONDEMNATION
- 602 ASSAULT AND BATTERY
- 604 MEDICAL MALPRACTICE
- 606 PRODUCT LIABILITY
- 607 PROFESSIONAL MALPRACTICE
- 608 TOXIC TORT
- 609 DEFAMATION
- 616 WHISTLEBLOWER / CONSCIENTIOUS EMPLOYEE PROTECTION ACT (CEPA) CASES
- 617 INVERSE CONDEMNATION
- 618 LAW AGAINST DISCRIMINATION (LAD) CASES

Track IV - Active Case Management by Individual Judge / 450 days' discovery

- 156 ENVIRONMENTAL/ENVIRONMENTAL COVERAGE LITIGATION
- 303 MT. LAUREL
- 508 COMPLEX COMMERCIAL
- 513 COMPLEX CONSTRUCTION
- 514 INSURANCE FRAUD
- 620 FALSE CLAIMS ACT
- 701 ACTIONS IN LIEU OF PREROGATIVE WRITS

Multicounty Litigation (Track IV)

271 ACCUTANE/ISOTRETINOIN	292 PELVIC MESH/BARD
274 RISPERDAL/SEROQUEL/ZYPREXA	293 DEPUY ASR HIP IMPLANT LITIGATION
281 BRISTOL-MYERS SQUIBB ENVIRONMENTAL	295 ALLODERM REGENERATIVE TISSUE MATRIX
282 FOSAMAX	296 STRYKER REJUVENATE/ABG II MODULAR HIP STEM COMPONENTS
285 STRYKER TRIDENT HIP IMPLANTS	297 MIRENA CONTRACEPTIVE DEVICE
286 LEVAQUIN	299 OLMESARTAN MEDOXOMIL MEDICATIONS/BENICAR
287 YAZ/YASMIN/OCELLA	300 TALC-BASED BODY POWDERS
289 REGLAN	601 ASBESTOS
290 POMPTON LAKES ENVIRONMENTAL LITIGATION	623 PROPECIA
291 PELVIC MESH/GYNECARE	

If you believe this case requires a track other than that provided above, please indicate the reason on Side 1, in the space under "Case Characteristics."

Please check off each applicable category

Putative Class Action

Title 59

LOCKS LAW FIRM, LLC

By: Michael A. Galpern, Esquire (Attorney No.: 029031988)
Andrew P. Bell, Esquire (Attorney No.: 025052010)
James A. Barry, Esquire (Attorney No.: 027512008)
801 N. Kings Highway
Cherry Hill, NJ 08034
Tel: (856) 663-8200

FILED & RECEIVED #1

2016 DEC 21 P 3:44

CIVIL OFFICE
MIDDLESEX VICINAGE

MORGAN & MORGAN COMPLEX LITIGATION GROUP

By: John A. Yanchunis, Esquire [To be admitted *Pro Hac Vice*]
Patrick Barthle, Esquire [To be admitted *Pro Hac Vice*]
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel.: (813) 223-5505

Attorneys for Plaintiff and the Putative Class

GRANT MORROW on behalf of himself and other persons similarly situated, Plaintiffs(s) v. QUEST DIAGNOSTICS INCORPORATED; JOHN DOES 1-99 (fictitious entities) and XYZ CORPORATIONS 1-99 (fictitious entities), Defendant(s)	SUPERIOR COURT OF NEW JERSEY LAW DIVISION: MIDDLESEX COUNTY DOCKET NO.: MID-L- 7406-16 Civil Action CLASS-ACTION COMPLAINT, DESIGNATION OF TRIAL COUNSEL AND DEMAND FOR JURY TRIAL
---	---

Plaintiff, Grant Morrow, by way of Complaint on behalf of himself and others similarly situated, individually and as class representative, upon information and belief, except for the allegations concerning Plaintiff's own actions, says as follows:

INTRODUCTION

1. This is a class-action Complaint brought by Plaintiff, Grant Morrow ("Plaintiff") on his own behalf and on behalf of all others similarly situated against Defendants Quest Diagnostics, Incorporated, John Does 1-99 (fictitious entities) and

XYZ Corporations 1-99 (fictitious entities)(hereafter “Defendants”), to obtain declaratory, injunctive and monetary relief for a class of individuals against Defendants for its failure to safeguard its client’s Protected Health Information (“PHI”) including laboratory test results and Personal Identifying Information (“PII”) including names, dates of birth, and phone numbers, which Defendants collected from Plaintiff and Class Members (collectively “Private Information”), and for failing to provide timely, accurate and adequate notice to Plaintiff and other Class Members that their Private Information had been stolen and failing to provide timely, accurate and adequate notice of precisely what types of information were stolen.

PARTIES

2. Plaintiff, Grant Morrow, is an adult individual residing in St. Petersburg Florida who was notified by letter dated December 12, 2016 from Quest Diagnostics that his Private Information was accessed by unauthorized persons. As a result of the breach, and the increased risk of identity theft caused by the breach, Mr. Morrow enrolled in an identity theft protection service at a monthly cost of \$14.95.

3. Defendant, Quest Diagnostics Incorporated (hereinafter “Quest”) is a business entity incorporated under the laws of Delaware with a headquarters located at Three Giralda Farms Madison, New Jersey 07940. Defendant operates laboratory locations throughout the State of New Jersey, including within Middlesex County with a laboratory location located at 92 Albany Street, Ground Floor, New Brunswick, New Jersey 08901.

4. Defendant John Does 1-99 (fictitious entities) are individuals, whose identities are currently unknown, who, along with Defendant Quest were responsible for the securing of Plaintiff and Class Member's Personal Information.

5. Defendant XYZ Corporations 1-99 (fictitious entities) are business entities, whose identities are currently unknown, which, along with Defendant Quest were responsible for the securing of Plaintiff and Class Members' Private Information.

FACTUAL ALLEGATIONS

A. Quest and the MyQuest by Care360 Service

6. Defendant Quest is a leading provider of diagnostic information services and laboratory testing, offering diagnostic testing for conditions as wide ranging as Allergy and Asthma testing, HIV testing, Ovarian Cancer Screening, Breast Cancer Screening, Celiac Disease Screening, Colorectal Cancer Screening, Hepatitis C testing, Prenatal Health (both prior to and during pregnancy), and Vitamin D testing.¹

7. Defendant offers consumers the MyQuest by Care360® internet application through (*inter alia*) its website, www.questdiagnostics.com where patients can view lab test results.

8. Defendant, in marketing the MyQuest by Care360® service touts not only the security of the service, but encourages consumers to add information to the PHI already on file with Defendant, including encouraging consumers to add insurance information, physician names, specialties and contact information, as follows:

Accessing your health information has never been easier. MyQuest delivers critical information directly to your computer, tablet and smart phone giving you the tools you

¹ Quest Diagnostics, Diagnostic Testing A-X, Available at <http://www.questdiagnostics.com/home/patients/tests-a-z.html>, last accessed December 19, 2016.

need to view, access and securely share your health information wherever you go...

Why make phone calls or wait for results by the mail? MyQuest delivers your results right to your smart phone, tablet or computer. MyQuest can access your results directly from the lab or from the physicians' offices who use Quest Diagnostics. Your lab report will include a brief explanation of the normal and abnormal values for each lab test to help you understand your results...

Just update MyQuest with details about your medical conditions and food and medication allergies. MyQuest securely stores all of your essential health information where you can always find it – on your smart phone, tablet or computer...

MyQuest gives you instant access to all of your healthcare resources. Manage physician names, specialties and contact information, hospital and pharmacy numbers, even insurance plan, group and policy numbers in MyQuest. This way, your vital information is always at your fingertips, whenever you need it...²

9. Defendant uses the MyQuest service to market products to physicians, particularly the Care360 EHR service, which it markets to physicians (and charges physicians a fee), noting at the time that it launched the MyQuest service that

The patient portal is also designed to help physicians that use the Quest Diagnostics Care360 Electronic Health Record (EHR) to qualify for the Centers for Medicare and Medicaid (CMS) EHR Incentive Program. Stage 2 of the MU program, which focuses on electronic engagement with patients, begins this year for providers that have participated in the program for at least two years. In order to meet the 2014 requirements of the CMS EHR Incentive Program, a physician must demonstrate that at least 50% of patients seen have online access to their health information (including lab results); 5% or more download, view or transmit their health information electronically; and 5% or more send the provider a secure electronic message.³

² <https://myquest.questdiagnostics.com/web/appts>, last visited December 19, 2016.

³ "Patients Nationwide Now Have Direct Access to Lab Test Results through Quest Diagnostics" Press Release, Quest Diagnostics, April 7, 2014. Available at:

Defendant thereby uses consumer's participation in the MyQuest by Care 360® system as a marketing tool to drive direct revenues through physician subscriptions to its Care360 EHR system.

10. Defendant's website, through which it offers the MyQuest services, provides: "This Web site can be accessed from the United States and other countries worldwide. Since the laws of each State or country may differ, you agree that the statutes and laws of the State of New Jersey, without regard to any principles of conflicts of law, will apply to all matters relating to the use of this site."⁴

11. Despite the fact that it was storing sensitive Private Information that it knew or should have known was valuable to and vulnerable to cyber attackers, Quest and its fellow Defendants failed to take adequate measures that could have protected user's Private Information.

12. On or about December 12, 2016 Defendant Quest announced that it on November 28, 2016 it became aware that it had suffered a data breach, in which an unauthorized third party accessed its MyQuest by Care360® internet application, obtaining the PHI of approximately 34,000 patients. Defendant indicted that the breach occurred "[o]n November 26th" but failed to provide the year of the access.

B. Consumers Rely on Quest's Private Information Security Practices

13. Quest maintains a Notice of Privacy Practices on its website ("Privacy Practices") which provides in relevant part:

⁴ Available at <http://www.questdiagnostics.com/home/privacy-policy/terms-conditions.html>, last visited December 19, 2016.

⁴ Available at <http://www.questdiagnostics.com/home/privacy-policy/terms-conditions.html>, last visited December 19, 2016.

Quest Diagnostics and its wholly owned subsidiaries (collectively "Quest Diagnostics") are committed to protecting the privacy of your identifiable health information. This information is known as "protected health information" or "PHI." PHI includes laboratory test orders and test results as well as invoices for the healthcare services we provide.

Our Responsibilities

Quest Diagnostics is required by law to maintain the privacy of your PHI. We are also required to provide you with this Notice of our legal duties and privacy practices upon request. It describes our legal duties, privacy practices and your patient rights as determined by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. We are required to follow the terms of this Notice currently in effect. We are required to notify affected individuals in the event of a breach involving unsecured protected health information. PHI is stored electronically and is subject to electronic disclosure. This Notice does not apply to non-diagnostic services that we perform such as certain drugs of abuse testing services and clinical trials testing services.⁵

14. In addition to the Privacy Practices, Quest maintains a Privacy Policy on its website ("Privacy Policy")⁶ which provides, in relevant part:

What Personal Information We Collect

Quest Diagnostics collects your personal information online when you voluntarily provide it to us. If you choose to register online, we ask you to provide limited personal information, such as your name, address, telephone number and/or email address. We also collect information that will allow you to establish a username and password if you would like to do that...

How We Use Personal Information That We Collect Online

Internal Uses

⁵ Available at <http://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html>, last visited December 19, 2016. (emphasis added)

⁶ Available at: <http://www.questdiagnostics.com/home/privacy-policy/online-privacy.html>, last visited December 19, 2016.

We may use your personal information within Quest Diagnostics: (1) to provide you with the services and products you request or that have been ordered and/or requested by your healthcare provider acting on your behalf; (2) to answer questions about our services; billing, payment methods or use of our website; (3) to process or collect payments for our services, (4) to conduct customer surveys; and (5) to contact you about the products and services that we offer.

Disclosure of Personal Information to Third Parties

We will not disclose any personal information to any third party (excluding our contractors to whom we may provide such information for the limited purpose of providing services to us and who are obligated to keep the information confidential), unless (1) you have authorized us to do so; (2) we are legally required to do so, for example, in response to a subpoena, court order or other legal process and/or, (3) it is necessary to protect our property rights related to this website.⁷ We also may share aggregate, non-personal information about website usage with unaffiliated third parties. This aggregate information does not contain any personal information about our users.

Cookie Placement

Certain Quest Diagnostics websites, like many other commercial sites, may use a standard technology called "cookies" to collect information about how our site is used. Cookies were designed to help a website operator determine that a particular user had visited the site previously and thus save and remember any preferences that may have been set. **We may use cookies to keep track of information about your current web browsing session which will be discarded as soon as you log out or close your web browser. This information also allows us to statistically monitor how many people are using our site and for what purpose. We may also make use of "persistent or memory based" cookies, which remain on your computer's hard drive until you delete them. An example of our use of these cookies is to pre-populate forms you complete on our website based on information you**

⁷ Emphasis added

have previously provided to us. [⁸] Although you have the ability to modify your browser to either accept all cookies, notify you when a cookie is sent, or reject all cookies, it may not be possible to utilize our services if you reject cookies.

Quest Diagnostics uses the services of Google Analytics, and may use other similar services, to collect and analyze statistical data about visitors to our website. We also use Google advertising services, and may use other similar services, to arrange for you to see Quest Diagnostics advertisements when you visit certain third party websites. These analytic and advertising services do not collect personally identifiable information. You may elect to opt out of the use of non-personally identifiable data by Google Analytics by downloading and installing an add-on to your web browser found [here](#). You may find out more about how Google Analytics collects and processes data by visiting "How Google uses data when you use our partners' sites or apps," found [here](#). You may also opt out of the Google AdWords service we use to serve ads, and which service also collects non-personally identifiable information, by visiting the Google Ad Settings page [here](#). For additional information about opting out of interest-based advertising, please visit [this page](#).

How We Protect Information Online

We exercise great care to protect your personal information. This includes, among other things, using industry standard techniques such as firewalls, encryption, and intrusion detection.[⁹]

15. Thus, Quest collects and stores massive amounts of PII in addition to PHI on its servicers and utilizes this information to maximize its profits.

16. Consumers place value in data privacy and security, and they consider it when making decisions regarding their online behavior, including signing up for an online medical records portal. Plaintiffs would not have utilized the MyQuest by Care

⁸ Emphasis added.

⁹ Emphasis added.

360® service had they known that Defendant did not take all necessary precautions to secure the personal data given to it by consumers.

17. Quest failed to disclose its negligent and insufficient data security practices and consumers relied on or were misled by this omission into using Defendants services.

18. The technology and medical industry is rife with similar examples of hackers targeting users' Private Information, including the hacks of Anthem¹⁰, Premera¹¹, and St. Joseph Health System¹² among others, all of which predate the time-frame Quest has identified regarding the Data Breach at issue in the present lawsuit.

19. As early as 2014 the FBI alerted healthcare firms that they were the target of hackers, stating "The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)"¹³.

C. Stolen Private Information Is Valuable to Hackers and Thieves

20. It is well known and the subject of many media reports that both Private Health Information and Personal Identify information is highly coveted and a frequent target of hackers. This information is targeted not only for identity theft purposes, but also for committing healthcare fraud, obtaining medical services under another's

¹⁰ Los Angeles Times, *Anthem is warning consumers about its huge data breach. Here's a translation*, March 6, 2015. Available at <http://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html>, last accessed December 19, 2016.

¹¹ New York Times, *Premera Blue Cross Says Data Breach Exposed Medical Data*, March 17, 2015. Available at http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html?_r=0, last accessed December 19, 2016.

¹² Napa Valley Register, *St. Joseph Health System sued for patient data breach*, April 9, 2012. Available at http://napavalleyregister.com/news/local/st-joseph-health-system-sued-for-patient-data-breach/article_948c0896-82a3-11e1-bed6-0019bb2963f4.html, last accessed December 19, 2012.

¹³ Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014. Available at <http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820>, last accessed December 19, 2016.

insurance. A study by Experian found that the “average total cost” of medical identity theft is “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.¹⁴ Despite well publicized litigation and frequent public announcements of data breaches by medical and technology companies, Quest opted to maintain an insufficient and inadequate system to protect the PHI and PII of Plaintiff and Class Members.

21. Legitimate organizations and the criminal underground alike recognize the value of PII. Otherwise, they wouldn’t aggressively seek or pay for it. For example, in “one of 2013’s largest breaches . . . not only did hackers compromise the [card holder data] of three million users, they also took registration data from 38 million users.”¹⁵ Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 users.

22. Biographical data is also highly sought after by data thieves. “Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts.” *Id.* PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of theft and unauthorized access have been the subject of many media reports. One form of identity theft, branded “synthetic identity theft,” occurs when thieves create new identities by combining real and fake identifying information and then use those identities to open new accounts.

¹⁴ Elinor Mills, *Study: Medical identity theft is costly for victims*, March 3, 2010, 5:00am PST. Available at: <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>, last accessed December 19, 2016.

¹⁵Verizon 2014 PCI Compliance Report, Available at http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter “2014 Verizon Report”), at 54 last visited December 19, 2016.

“This is where they’ll take your Social Security number, my name and address, someone else’s birthday and they will combine them into the equivalent of a bionic person,” said Adam Levin, Chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft, experts said: “It’s tougher than even the toughest identity theft cases to deal with because they can’t necessarily peg it to any one person.” In fact, the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number.

23. Unfortunately, and as is alleged below, despite all of this publicly available knowledge of the continued compromises of Personal Identifying Information in the hands of third parties, such as health companies, Quest’s approach at maintaining the privacy of the Plaintiff’s and the Class Members’ PII and PHI was lackadaisical, cavalier, reckless, or at the very least negligent.

D. This Data Breach Will Result in Additional Identity Theft and Identity Fraud.

24. Quest failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Identifying Information and Private Health Information maintained on its systems.

25. The ramifications of Quest’s failure to keep Plaintiff’s and Class Members’ data secure are severe. As explained by the Federal Trade Commission:

Medical identity theft happens when someone steals your personal information and uses it to commit health care fraud. Medical ID thieves may use your identity to get treatment — even surgery — or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft

can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.¹⁶

26. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."¹⁷

27. According to Javelin Strategy and Research, "1 in 4 notification recipients became a victim of identity fraud."¹⁸

28. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."¹⁹ In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id.* at 11.

29. Javelin Strategy and Research reports that losses from identity theft increased to \$21 billion in 2013.²⁰

30. There may be a time lag between when harm occurs and when it is

¹⁶ Federal Trade Commission, *Medical ID Theft: Health Information for Older People*, available at <https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people>, last accessed December 19, 2016.

¹⁷ Federal Trade Commission, *Warning Signs of Identity Theft*, available at <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft>, last accessed December 19, 2016.

¹⁸ See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at www.javelinstrategy.com/brochure/276, last visited December 19, 2016 (the "2013 Identity Fraud Report").

¹⁹ Victims of Identity Theft, 2012 (Dec. 2013) at 10, available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf>, last accessed December 19, 2016.

²⁰ See 2013 Identity Fraud Report.

discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²¹

31. Plaintiff and Class Members now face years of constant surveillance of their financial, personal and medical records. The Class is incurring and will continue to incur such damages in addition to any fraudulent charges made to their financial accounts or medical insurance, whether or not such charges are ultimately reimbursed by the credit card companies.

E. Plaintiff and Class Members Suffered Damages

32. The Data Breach was a direct and proximate result of Quest’s failure to properly safeguard and protect Plaintiff’s and Class Members’ Private Identifying Information and Private Health Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Quest’s failure to establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Plaintiff’s and Class members’ Personal Identifying Information and Personal Health Information to protect against reasonably foreseeable threats to the security or integrity of such information.

²¹ GAO, Report to Congressional Requesters, at p.33 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (emphases added) (last visited Sept. 24, 2014).

33. Plaintiff's and Class Members' Personal Identifying Information and Private Health Information is private and sensitive in nature and was left inadequately protected by Quest. Quest did not obtain Plaintiff's and Class Members' consent to disclose either their Personal Identifying Information or their Private Health Information to any other person as required by applicable law and industry standards.

34. As a direct and proximate result of Quest's wrongful action and inaction and the resulting Data Breach, Plaintiff (as addressed above) and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take time and effort to mitigate the actual and potential impact of the Data Breach on their lives by, among other things, placing "freezes" or "alerts" with credit reporting agencies, contacting their health insurance providers, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their medical "explanations of benefits" and credit reports and accounts for unauthorized activity.

35. Quest's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members Private Health Information and Personal Identifying Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation including:

- a. Theft of their personal, medical, and/or financial information;
- b. The reputational harms suffered by Defendant's publication of private facts in the form of Plaintiff's and Class Members' medical records;

- c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal and medical information being placed in the hands of criminals;
- d. The untimely and inadequate notification of the Data Breach;
- e. The improper disclosure of Plaintiff's and Class Member's private information;
- f. Loss of Privacy;
- g. Ascertainable loss in the form of out-of pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.
- h. Ascertainable losses in the form of deprivation of the value of their Personal Identifying Information and Private Health Inforamtion, for which there is a well-established national and international market;
- i. overpayments to Quest for products and services in that a portion of the price paid for such products and services by Plaintiffs and Class members to Quest was for the costs of reasonable and adequate safeguards and security measures that would protect users' Private Information, which Quest did not implement and, as a result, Plaintiffs and Class members did not receive what they paid for and were overcharged by Quest;

CLASS ACTION ALLEGATIONS

36. This action is brought and may properly proceed as a class action, pursuant to the provisions of Rule 4:32 of the New Jersey Court Rules. Plaintiffs bring this action on behalf of themselves and all others similarly situated. Plaintiffs seek certification of a Class, initially defined as follows:

All persons residing in the United States whose personal information was disclosed in the Data Breach announced by Quest on or about December 12, 2016.

37. The Class and Subclass for those whose benefit this action has been brought is so numerous that joinder of all members is impracticable, as Defendant has indicated it believes as many as 34,000 individuals may have been impacted in the Breach.

38. Plaintiff's claims are typical of the claims of the members of the Class, since all such claims arise out of Defendant's failure to safeguard user's information and by Defendant's own terms of service every Class Member will be subject to New Jersey law.

39. Plaintiff does not have interests antagonistic to the interests of the Class or Subclass.

40. The Class and Subclass, of which Plaintiff is a member, are readily identifiable by reference to Defendant's records.

41. Plaintiff will fairly and adequately protect the interests of the Class and Subclass and have retained competent counsel experienced in the prosecution of consumer litigation. Proposed Class Counsel has investigated and identified potential claims in the action; has a great deal of experience in handling class actions, other complex litigation, and claims of the type asserted in this action.

42. There are common questions of law and fact effecting the rights of all class members, including the following:

- a. Whether Quest violated New Jersey law by failing to implement reasonable security measures;
- b. Whether Quest violated common and statutory law by failing to promptly notify Class Members their Private Health Information and Personal Identifying Information had been compromised;
- c. Whether class members may obtain injunctive relief against Quest under New Jersey law to require that it safeguard or destroy, rather than retain as it has the Private Health Information and Personal Identifying Information of Plaintiff and the Class Members;
- d. Which security procedures and which data-breach notification procedure Quest should be required to implement as part of any injunctive relief ordered by the Court;
- e. Whether Quest has contractual obligations to use reasonable security measures;
- f. Whether Quest has complied with contractual obligations to use reasonable security measures;
- g. What security measures, if any, must be implemented by Yahoo to comply with its contractual obligations;
- h. Whether Quest has implied contractual obligations to use reasonable security measures;

- i. Whether Quest has complied with implied contractual obligations to use reasonable security measures;
- j. What security measures, if any, must be implemented by Yahoo to comply with its implied contractual obligations;
- k. Whether Quest violated New Jersey privacy laws in connection with the actions described here; and
- l. What the nature of the relief should be, including equitable relief, to which Plaintiff and Class Members are entitled.

43. A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. While the economic damages suffered by the individual Class Members are significant, the amount is modest compared to the expense and burden of individual litigation. A class action will cause an orderly and expeditious administration of the claims of the Class and will foster economies of time, effort and expense.

44. The questions of law and/or fact common to the members of the Class predominate over any questions affecting only individual members.

45. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for the Defendant in this action or the prosecution of separate actions by individual members of the Class would create the risk that adjudications with respect to individual members of the Class and Subclass would as a practical matter be dispositive of the interests of the other members not parties to the

adjudications or substantially impair or impede their ability to protect their interests.

Prosecution as a class action will eliminate the possibility of repetitious litigation.

46. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the class as a whole.

47. Plaintiffs do not anticipate any difficulty in the management of this litigation.

COUNT ONE

**Negligence
(As to Plaintiff and the Class)**

48. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

49. Defendant, through the course of providing services to Plaintiff and the Class, obtained their Private Information.

50. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII and PHI of Plaintiff and Class Members.

51. Upon accepting and storing Plaintiff's and Class Members' PHI and PII in their computer database systems, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Quest knew, acknowledged, and agreed that the Plaintiff and Class Member's PHI AND PII was private and confidential and would be protected as private and confidential.

52. Defendant breached their duties of care to Plaintiff and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiffs' PHI and PII.

53. Defendant acted with wanton disregard for the security of Plaintiff and Class Members' PHI and PII. Defendant knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the PHI and PII in health care databases such as Quest's.

54. The law imposed an affirmative duty on Quest to timely discover and disclose the unauthorized access and theft of the PHI and PII to Plaintiffs and the Class so that Plaintiffs and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

55. To date, Quest has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

56. Defendant also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard Plaintiff and Class Members' information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Quest failed to provide adequate supervision and oversight of the Private Information with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather

Plaintiffs' and Class Members' Private Information, misuse the Private Information, and intentionally disclose it to others without consent.

57. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen, and misused, Quest unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' Private Information during the time it was within Quest's possession or control.

58. Further, through its failure to timely discover and provide clear notification of the Data Breach to consumers, Quest prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their Private Information.

59. Upon information and belief, Quest improperly and inadequately safeguarded the Private Information of Plaintiffs and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

60. Defendant's failure to take proper security measures to protect Plaintiff's and Class Members' sensitive Private Information as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' Private Information.

61. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information; failing to conduct adequate regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class Members' Private Information; and failing to provide Plaintiffs and Class Members

with timely and sufficient notice that their sensitive Private Information had been compromised.

62. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

63. As a direct and proximate cause of Defendant's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT TWO

Breach of Contract (On Behalf of Plaintiff and the Class)

64. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

65. As set forth above, Plaintiff and Class Members who received laboratory services from Defendant and/or enrolled in the MyQuest by Care360® service.

66. As set forth above, the contract between Plaintiff and Class members and Quest was supported by consideration in many forms including the payment of monies for laboratory testing services, and/or the enrollment in Defendant's service, which permitted Defendant to market its paid Physician services.

67. Plaintiff and Class Members performed pursuant to these contracts, and satisfied all conditions, covenants, obligations, and promises of the agreements.

68. Under the contracts, Defendant was obligated, as outlined in the Privacy Practices and Privacy Notices, to maintain the confidentiality of Plaintiff and Class Member's PHI and PII.

69. As a result of Defendant's breach of contract, by failing to adequately secure Plaintiff and Class Member's PHI and PII, Plaintiff and Class members did not receive the full benefit of the bargain, and instead received services that were less valuable than described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in value between what was promised and what Quest ultimately provided.

70. Also as a result of Quest's breach of contract, Plaintiff and Class Members have suffered actual damages resulting from the theft of their PHI and PII, and remain at imminent risk of suffering additional breaches in the future.

COUNT THREE

Breach of Implied Contract (On Behalf of Plaintiff and the Class)

71. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

72. Quest solicited and invited Plaintiff and Class Members to use its services. Plaintiff and Class Members accepted Quest's offers and created user accounts requiring the provision of PHI and PII with Quest.

73. When Plaintiff and Class Members used Quest services and products, they provided their PHI and PII. In so doing, Plaintiffs and Class Members entered into

implied contracts with Quest pursuant to which Quest agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised.

74. Each use of a Quest service or product made by Plaintiff and Class Members was made pursuant to the mutually agreed-upon implied contract with Quest under which Yahoo agreed to safeguard and protect Plaintiff's and Class Members' PHI and PII and to timely and accurately notify them if such information was compromised or stolen.

75. Plaintiff and Class Members would not have provided and entrusted their PHI and PII to Quest in the absence of the implied contract between them and Quest.

76. Plaintiff and Class Members fully performed their obligations under the implied contracts with Quest.

77. Quest breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the PHI and PII of Plaintiff and Class Members and by failing to provide timely and accurate notice to them that their Private Information was compromised in and as a result of the Data Breach.

78. As a direct and proximate result of Quest's breaches of the implied contracts between Quest and Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages as described in detail above.

COUNT FOUR

Publication of Private Facts (On Behalf of Plaintiff and the Class)

79. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

80. Defendant, by and through its failure to adequately safeguard Plaintiff and Class Member's PHI and PII has made Plaintiff and Class Member's information public.

81. Plaintiff and Class Member's private medical results, lists of treating doctors and other sensitive information were private, as Defendant acknowledged as aforesaid.

82. Dissemination of information such as the PHI and PII revealed by Defendant about Plaintiff and Class Members would be offensive to a reasonable person.

83. Plaintiff and other Class Member's PHI and PII is not of legitimate public concern, and there is no legitimate public interest in the public being apprised of said information.

84. Plaintiff and other Class Members did not consent to the disclosure of their PHI and PII.

85. As a direct and proximate result of Quest's breaches of the implied contracts between Quest and Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages as described in detail above. Additionally Plaintiff and Class members are entitled to presumed damages as a result of Defendant's publication of private facts.

COUNT FIVE

Unjust Enrichment
(On Behalf of Plaintiff and the Class)

86. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

87. In the alternative to the above plead claims, Plaintiff and the Class allege that they have no adequate remedy at law and bring this unjust enrichment claim.

88. Plaintiff and Class Members conferred a monetary benefit on Defendant Quest, by their participation in the MyQuest program, which Defendant utilized to market its pay services to physicians as explained above.

89. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members.

90. The amounts paid to Defendant (partially) as a result of Plaintiff and Class Members' participation in the MyQuest program should have been used by Defendant in part to pay for the administrative costs of reasonable data privacy and security practices and procedures.

91. As a result of Defendant's conduct, Plaintiff and Class members suffered actual damages as aforesaid.

92. Under principals of equity, Defendant should not be permitted to retain the money it collected as a result of Plaintiff and Class Members' participation in the MyQuest program because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members were fairly entitled, and which were otherwise mandated by HIPAA regulations, federal, state and local laws, as well as industry standards.

93. Quest should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by Quest.

COUNT SIX

Violation of the NJ Consumer Fraud Act, N.J.S.A. 56:8-1, *et seq.* (On Behalf of Plaintiff and the Class)

94. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

95. Plaintiffs and the Class bring these claims against Defendant under the New Jersey Consumer Fraud Act.

96. Defendant sells "merchandise" as defined by the New Jersey Consumer Fraud Act by offering health services to the public as well as the MyQuest service to consumers.

97. Defendant engaged in unconscionable and deceptive acts and practices, misrepresentation and the concealment, suppression and omission of material facts with respect to the sale and advertisement of their services in violation of *N.J.S.A. 56:8-2*, including by not limited to the following:

- a. Misrepresenting material facts, pertaining to their services to consumers by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Class Members' PHI and PII from unauthorized disclosure, release, data breaches and theft;
- b. Misrepresenting material facts by representing to Plaintiff and Class members that they did and would continue to comply with the relevant industry data security standards, state law and federal law with regard to the protection of Plaintiff and Class Members' PHI and PII;
- c. Defendant knowingly omitted, suppressed and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and the Class Members' PHI and PII with the intent that Plaintiff and the Class Members would rely on the omission, suppression and concealment;

d. Defendant engaged in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiff and Class Members in a timely and accurate manner in violation of *N.J.S.A. 56:8-163(a)*.

98. As a direct and proximate result of Defendant's unconscionable or deceptive acts and practices, Plaintiff and Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PHI and PII.

99. Plaintiff and Class members are therefore entitled to injunctive relief, equitable relief, actual damages, treble damages, and attorneys' fees and costs pursuant to *N.J.S.A. 56:8-19*.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against Quest as follows:

- a. For an Order certifying the Class as defined here, and appointing Plaintiff and his Counsel to represent the Class;
- b. For equitable relief enjoining Quest from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff and Class Members' Private Health Information and Personal Identifying Information, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class Members;
- c. For equitable relief compelling Quest to utilize appropriate methods and policies with respect to consumer data collection, storage, and

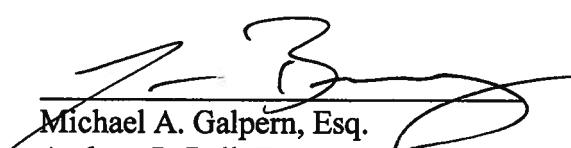
safety and to disclose with specificity to Class Members the type of Private Health Information and Personal Identifying Information compromised.

- d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Quest's wrongful conduct;
- e. For an award of actual damages and compensatory damages, in an amount to be determined;
- f. For an award of treble damages, as allowable by law;
- g. For an award of costs of suit and attorneys' fees, as allowable by law; and
- h. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

LOCKS LAW FIRM, LLC



Michael A. Galpern, Esq.
Andrew P. Bell, Esq.
James A. Barry, Esq.
801 N. Kings Highway
Cherry Hill, NJ 08034
Tel: (856) 663-8200
Fax: (856) 661-8400

**MORGAN & MORGAN
COMPLEX LITIGATION GROUP**
John A. Yanchunis, Esq. [To be admitted *Pro Hac Vice*]
Patrick Barthle, Esq. [To be admitted *Pro Hac Vice*]
201 Franklin Street, 7th Floor

Tampa, Florida 33602
Tel.: (813) 223-5505
Fax: (813) 334-5402

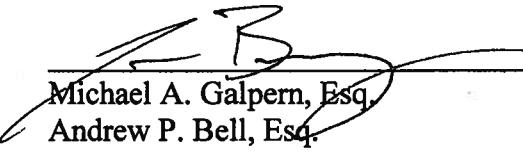
Attorneys for Plaintiff and the Putative Class

Dated: December 21, 2016

CERTIFICATION PURSUANT TO RULE 4:5-1 and N.J.S.A. 56:8-1 et. seq.

1. I hereby certify that to my knowledge the matter in controversy is not the subject of any other action pending in any court or of a pending arbitration.
2. To my knowledge, no other action or arbitration procedure is contemplated.
3. I have no knowledge at this time of the names of any other parties who should be joined in this action.
4. I have forwarded a copy of this Complaint to the Attorney General of the State of New Jersey and Middlesex County Office of Consumer Affairs pursuant to *N.J.S.A. 56:8-1, et seq.*

LOCKS LAW FIRM, LLC



Michael A. Galpern, Esq.
Andrew P. Bell, Esq.
James A. Barry, Esq.
801 N. Kings Highway
Cherry Hill, NJ 08034
Tel: (856) 663-8200
Fax: (856) 661-8400

**MORGAN & MORGAN
COMPLEX LITIGATION GROUP**
John A. Yanchunis, Esq. [To be admitted *Pro Hac Vice*]
Patrick Barthle, Esq. [To be admitted *Pro Hac Vice*]
201 Franklin Street, 7th Floor
Tampa, Florida 33602
Tel.: (813) 223-5505
Fax: (813) 334-5402

Attorneys for Plaintiff and the Putative Class

Dated: December 21, 2016